Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Policy on Management of Information Technology.

Published: 2018-04-01

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board, 2018

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT48-14/2018E-PDF
ISBN: 978-0-660-26140-9

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Politique sur la gestion des technologies de l'information.

Policy on Management of Information Technology

1. Effective date

1.1 This policy takes effect on July 1, 2007, and incorporates updates effective April 1, 2018.

2. Application

2.1 This policy applies to departments as defined in section 2 of the Financial Administration Act, unless excluded by specific acts, regulations, or Orders in Council.

2.2 The following sections do not apply with respect to the Office of the Auditor General, the Office of the Privacy Commissioner, the Office of the Information Commissioner, the Office of the Chief Electoral Officer, the Office of the Commissioner of Lobbying, the Officer of the Commissioner of Official Languages and the Office of the Public sector Integrity Commissioner: 6.1.5, 6.1.6, 6.1.9, 6.1.12, 6.2.10 to 6.2.13, 6.2.15, 6.4.6, 6.4.8, 6.4.10, 6.4.12, 6.5.3 and 7.1. The deputy heads of these organizations are solely responsible for monitoring and ensuring compliance with this policy within their organizations, as well as for responding to cases of non-compliance in accordance with any Treasury Board instruments that address the management of compliance.

2.3 Section 6.2.10 does not apply to small departments and agencies.

2.4 This policy does not apply to National Security Systems, except where the Government of Canada Chief Information Officer is identified as the system business owner.

3. Context

3.1 Information technology (IT) plays an important role in government operations. It is also a key enabler in transforming the business of government. Information technology is an essential component of the government's strategy to address

challenges of increasing productivity and enhancing services to the public for the benefit of citizens, businesses, taxpayers and employees.

3.2 Deputy heads are responsible for the effective management of IT within their departments, including the implementation of IT spending decisions and ensuring appropriate, ongoing measurement of IT performance.

3.3 This policy is issued pursuant to section 7 of the Financial Administration Act and section 31 of the Public Service Employment Act.

3.4 This policy is to be read in conjunction with the Policy Framework on Information and Technology and supporting directives and standards.

3.5 The Treasury Board has delegated to the Secretary of Treasury Board the authority to issue directives and associated standards in the areas of IT governance and IT strategies to support this policy and, in executing these functions, the Secretary will be supported by the Chief Information Officer of the Government of Canada.

3.6 Additional mandatory requirements will be set out in directives and standards in the areas of IT governance and IT strategies.

4. Definitions

4.1 Definitions to be used in the interpretation of this policy are in the Appendix.

5. Policy statement

5.1 **Objective**

5.1.1 The governance and oversight of Information Technology (IT) investments and management in the Government of Canada (GC) is strengthened;

5.1.2 IT services are responsive to GC priorities, program delivery and business needs; and

5.1.3 IT services address barriers to engagement with Canadians while meeting their changing needs;

5.1 **Expected results**

The expected results of this policy are:

- a better understanding on the part of all key stakeholders of their roles and responsibilities with respect to the management of IT in the government;
- strengthened management of IT across the government and better decision-making at all levels, thus ensuring that IT supports program delivery and provides value for money;
- increased use of common or shared IT assets and services by departments and agencies to ensure efficiency gains;
- IT services investments and management are efficient and effective;
- IT services are innovative, resulting in excellence in service and end-user experience;
- Cyber security is strengthened government-wide; and
- Chief Information Officers (CIO) participate in senior executive governance, strengthening the business and IT partnership.

6. Policy requirements

6.1 **Deputy heads are responsible for the following:**

Governance and oversight

6.1.1 Ensuring the efficient and effective governance and oversight of IT within their departments, including IT investment decisions, ongoing management, compliance with policy, standards and directives, performance measurement, and relevant collective agreement provisions;

6.1.2 Ensuring the departmental IT investment plan is integrated into the overall departmental business plans;

6.1.3 Investigating and taking appropriate and timely actions when significant issues regarding Policy on Management of Information Technology compliance arise within the department;

6.1.4 Ensuring departmental participation in setting GC IT strategic direction;

6.1.5 Ensuring compliance with procedures established for accessing alternative service delivery mechanisms to SSC, as necessary;

6.1.6 Ensuring that enterprise or shared IT assets and services are used in departments to avoid duplication, when such assets and services are available and appropriate;

6.1.7 Approving the annual three-year forward-looking departmental IT Plan, which may be included as part of an integrated information management and information technology plan;

6.1.8 Ensuring that the Treasury Board of Canada Secretariat is informed of their activities in relation to this policy that involve the development of national and international standards;

IT workforce management

6.1.9 Ensuring that a senior official is designated as the Chief Information Officer (CIO) for the purposes of this policy;

6.1.10 Ensuring the development of talent management and succession plans that:

6.1.10.1 Demonstrate that the department has ongoing strategic leadership capabilities and the capacity to lead the IT management workforce; and

6.1.10.2 Support the Chief Information Officer of the Government of Canada's government-wide talent management and community development initiatives;

6.1.11 Ensuring that the CIO has direct access on a periodic basis to their deputy head.

6.1.12 Consulting with the Secretary of the Treasury Board regarding creating a departmental CIO position, and prior to the appointment, deployment, replacement or departure of a departmental CIO.

6.1.13 Ensuring that, for the purposes of the Treasury Board Executive Group (EX) Qualifications Standard, the CIO possesses an acceptable combination of education, training and/or experience as determined by the Chief Information Officer of the Government of Canada.

6.2 Departmental Chief Information Officers are responsible for the following:

Departmental IT

6.2.1

Providing strategic IT advice and acting as an effective business partner in advancing departmental priorities by providing leadership on information technology support to senior departmental officials;

6.2.2 Approving the IT component of all departmental strategies, plans, initiatives, projects, procurements, and spending authority requests;

6.2.3 Providing efficient and effective IT services that are responsive to departmental priorities, program delivery and business needs;

6.2.4 Ensuring that departmental data and applications, as well as departmental systems and networks (where these services are not provided by SSC), are secure, reliable and trusted;

6.2.5 Undertaking immediate action within the department at the direction of the Chief Information Officer of the Government of Canada to assess impacts and implement security controls in response to cyber security events, including incidents and vulnerabilities;

6.2.6 Supporting the use of cloud services first by ensuring that:

6.2.6.1 Cloud services are identified and evaluated as a principal delivery option when initiating new departmental, enterprise, and community of interest cluster IT investments, initiatives, strategies and projects;

6.2.6.2 Cloud services are adopted when they are the most effective option to meet business needs; and

6.2.6.3 Adopted cloud service(s) fully comply with appropriate privacy and security standards;

6.2.7 Ensuring that all sensitive electronic data under government control, that has been categorized as Protected B, Protected C or is Classified, will be stored in a GC-approved computing facility located within the geographic boundaries of Canada or within the premises of a GC department located abroad, such as a diplomatic or consular mission. This does not mean that the country of origin of IT service providers must be Canada, as long as these service providers can ensure storage of data within boundaries or premises as described above.

6.2.8

Ensuring that all newly procured or developed IM/IT solutions and equipment meet or exceed applicable requirements or standards for persons with disabilities and official languages;

6.2.9 Ensuring decisions and actions regarding IT are guided by the GC annual strategic plan on IT, the Chief Information Officer of the Government of Canada's prioritization of GC demand for IT services and assets, and IT Policy Implementation Notices, and compliant with policy, directives, standards , and relevant collective agreement provisions;

6.2.10 Chairing a departmental architecture review board that is mandated to review and approve the architecture of all departmental IT services, projects, initiatives, procurements and strategies, and ensures their alignment with GC government-wide architectures;

6.2.11 Developing, in line with the Chief Information Officer of the Government of Canada's government-wide IT talent management and community development initiatives, the capacity and capability of the departmental IT workforce to meet departmental IT requirements.

Government-wide IT

6.2.12 Aligning departmental IT priorities and strategies with government-wide IT priorities and strategies;

6.2.13 Participating in and supporting government-wide IT initiatives and projects that contribute to the strategic and business goals of the department and the GC; and,

6.2.14 Identifying emerging technologies that could potentially contribute to the strategic and business goals of the department and the GC;

IT Information

6.2.15 Producing the departmental IT Plan and IT progress report, the IT expenditure report, and responding to compliance monitoring and performance measurement processes and on-going Application Portfolio Management update reports.

6.3 The Secretary of the Treasury Board is responsible for the following:

6.3.1

Chairing a deputy head level IT governance and management committee which is responsible for providing counsel to the Chief Information Officer of the Government of Canada on setting strategic direction, the prioritization of GC demand for IT services and assets, and identifying emerging technologies.

6.4 **The Chief Information Officer of the Government of Canada is responsible for the following, which will be exercised in accordance with a sub-delegation from the Secretary of the Treasury Board where required:**

6.4.1 Providing strategic advice to the Secretary of the Treasury Board and, through the Secretary, to the President of the Treasury Board and to the Clerk of the Privy Council, and GC-wide direction and advice to departmental deputy heads and CIOs, on the management of IT within the GC, including on the strategic direction of GC IT, the prioritization of GC demand for IT shared services and assets, and emerging technologies and implications and opportunities for the Government of Canada;

6.4.2 Developing an annual strategic plan on IM and IT to establish government-wide IT priorities that are strategically aligned to address the Government of Canada's business priorities;

6.4.3 Establishing priorities among the IT investments (including cyber security investments) that are enterprise in nature or require the support of Shared Services Canada as advised and endorsed by the appropriate Deputy Minister level governance committee;

6.4.4 Supporting the development and implementation, by Shared Services Canada (SSC), of procedures for accessing and assessing alternative service delivery mechanisms to SSC, to support the authority of the Minister responsible for SSC;

6.4.5 Providing advice to the President of the Treasury Board to support Treasury Board's review and approval of the annual SSC Investment Plan to ensure alignment with established strategic direction and enterprise priorities, as well as in assessing progress;

6.4.6 Prescribing government-wide architecture expectations and establishing and implementing an enterprise architecture review board that is mandated to define current and target architecture standards for the

Government of Canada, and review departmental plans to ensure alignment;

6.4.7 Prescribing the use of specific business processes, technologies, applications and IT resource management approaches;

6.4.8 Providing GC-wide direction for IT solution procurement that maximizes flexibility for the GC;

6.4.9 Establishing guidance to support innovative practices and technologies, including open source and open standard applications, and agile application development;

6.4.10 Monitoring, providing guidance and recommending corrective actions regarding the following:

6.4.10.1 Compliance with this policy and its supporting instruments;

6.4.10.2 IT management performance of departments; and

6.4.10.3 The IT management function across government;

6.4.11 Executing cyber security risk management decisions on behalf of the GC and directing a Deputy Head to implement a specific response to cyber security events, including the implementation of security controls and ensuring that systems that put the GC at risk are disconnected or removed, when warranted;

6.4.12 When acting as the business owner, ensuring the efficient and effective governance and oversight of enterprise IT initiatives, including investment decisions, ongoing management, compliance with policy, standards and directives, performance measurement and relevant collective agreement provisions; and,

6.4.13 Working with departments in reviewing and endorsing IT initiatives, projects and investments, and reviewing results and benefits realized.

IT workforce

6.4.14 Providing government-wide functional leadership regarding the following:

6.4.14.1 Knowledge standards for the IT community, including determining the acceptable combination of education, training

and/or experience for purposes of the Treasury Board Executive Group (EX) Qualification Standard; and

6.4.14.2 Development and sustainability of the IT community through talent management and community development strategies.

6.5 Monitoring and reporting requirements

Deputy heads

6.5.1 Deputy heads are responsible for monitoring adherence to this policy within their departments, consistent with the provisions of the Treasury Board's Policy on Results and Policy on Internal Audit, and for ensuring that appropriate remedial action is taken to address any deficiencies within their departments.

6.5.2 Deputy heads with national or policy responsibilities related to information technology are responsible for providing to the Treasury Board of Canada Secretariat, on an annual basis, the names and responsibilities of their officers who are involved in national and international IT standards activities, to ensure a comprehensive understanding of the Government of Canada's involvement and contribution.

Government-wide

6.5.3 The Treasury Board of Canada Secretariat will monitor IT management performance of departments, the IT management function across government, and compliance with this policy in a variety of ways, including but not limited to, the following:

- assessments under the Management Accountability Framework;
- examinations of Treasury Board submissions, departmental performance reports, results of audits, evaluations and studies; and
- work performed in collaboration with departments.

6.5.4 Treasury Board of Canada Secretariat will review this policy, its associated directives and standards, and their effectiveness at the five year mark of implementation of the Policy (or earlier for certain directives and standards). When substantiated by risk-analysis, the Treasury Board of Canada Secretariat will also ensure an evaluation is conducted.

6.5.5 The Treasury Board of Canada Secretariat will monitor government-wide progress against established strategic IT directions and will measure government-wide IT performance on an ongoing basis.

7. Consequences

7.1 Consequences of non-compliance can include informal follow-ups and requests from Treasury Board of Canada Secretariat, external audits, and formal direction on corrective measures.

7.2 Consequences of non-compliance with this policy can include any measure allowed by the Financial Administration Act that the Treasury Board would determine as appropriate and acceptable in the circumstances.

8. Roles and responsibilities of other government departments

Note: This section identifies other departments who have a role in the management of IT. In and of itself, this section does not confer an authority.

The Canada School of Public Service is responsible for the development and delivery of a government wide core learning strategy and program for all public service employees involved in the management of IT in consultation with the relevant functional authority centres and consistent with the Policy on Learning, Training and Development.

Public Services and Procurement Canada is responsible for providing services for federal departments and agencies, to support them in the achievement of their mandated objectives as their central purchasing agent, linguistic authority, real property manager, treasurer, accountant, integrity adviser, and pay and pension administrator.

Public Works and Government Services Canada is responsible for the management and operation of the common and shared IT services in consultation with departments and the Treasury Board of Canada Secretariat.

Shared Services Canada is responsible for providing certain services related to email, data centres, networks and end-user technology devices. Use of SSC services is required for specified government departments; however other departments and agencies may also choose to use these services. Whenever possible, SSC is responsible for delivering these services in a consolidated and standardized manner. Some of SSC's services are provided on a cost-recovery basis. SSC also provides government-wide operational

coordination of cyber security events, including IT incident response and recovery, and supports government-wide decision-making with respect to incident mitigation. In exceptional circumstances, the Minister responsible for SSC can personally authorize a department to provide itself with otherwise mandatory services (or obtain them from a third party).

Treasury Board of Canada Secretariat is responsible for establishing the overall government-wide strategic directions for IT in consultation with deputy heads; identifying areas that offer significant government-wide benefits or are of importance to the government; and leading initiatives to achieve government-wide solutions and the implementation of government-wide directions with the appropriate common service or shared service organizations that are of importance to the government.

The Communications Security Establishment (CSE) is the lead technical authority for information technology (IT) security including the provision of leadership, advice and guidance for technical matters related to information technology (IT) security. It helps ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada, and fulfils government-wide functions by identifying emerging cyber threats, monitoring government networks and systems, and helping to protect against, and mitigate potential impacts of cyber security events. CSE leads the development of trusted sources of supply for government and critical infrastructure alongside mitigating the risk of untrusted equipment. CSE is the national authority for communications security (COMSEC), including the procurement, distribution, control and use of cryptographic devices and encryption keying material for national security systems. CSE is also Canada's national authority for signals intelligence (SIGINT).

9. References

9.1 Treasury Board policies

- Common Services Policy
- Policy on Communications and Federal Identity
- Policy on Government Security
- Policy on Results
- Policy on Information Management
- Policy on Internal Audit
- Policy on Official Languages
- Policy on Learning, Training and Development
- Policy on Investment Planning – Assets and Acquired Services

- Policy on Management of Materiel
- Policy on Service
- Policy on the Duty to Accommodate Persons with Disabilities in the Federal Public Service
- Policy on Privacy Protection
- Policy on the Management of Projects

9.2 Other publications

- An Enhanced Framework for the Management of Information Technology Projects
- Management Accountability Framework (MAF)

10. Enquiries

Please direct enquiries about this policy to the senior official appointed by your deputy head for the purposes of this policy. For interpretation of this policy, this senior official should contact:

Chief Information Officer Branch
Treasury Board of Canada Secretariat
Ottawa ON K1A 0R5
E-mail: Cio-dpi@tbs-sct.gc.ca

Appendix - Definitions

Client (client)

The intended recipient of a service. Clients may be external (citizens, businesses, non-Canadians, or organizations, e.g., non-profit) or internal to government (departments).

Common service (service commun)

A service that is provided by a common service organization.

Common service organization (organisme de services communs)

A department or organization that is designated as a central supplier of particular services to support the requirements of departments. Common service organizations are listed in Appendix B of the Common Services Policy.

Cyber Security (Cybersécurité)

The body of technologies, processes, practices and response and mitigation measures designed to protect electronic information and information infrastructure from mischief, unauthorized use, or disruption.

Information technology (technologies de l'information)

Includes any equipment or system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes all matters concerned with the design, development, installation and implementation of information systems and applications to meet business requirements.

Management of information technology (gestion des technologies de l'information)

Includes planning, building (or procuring), operating and measuring performance.

National Security System (système national de sécurité)

A Canadian National Security System is a system within which national security activities are enabled and protected, and information, resources and assets are of such sensitivity that compromise could undermine the national security of Canada or its partners. The security measures required for a national security system are designed to provide confidence and defense against the most sophisticated threats.

Service (service)

A means, administered by a program, of producing a final valued output (i.e. service output) to address one or more target group needs.

Shared service (Service partagé)

A service that is shared by more than one client.

Small departments and agencies (Petits ministères et organismes)

Organizations that have reference levels including revenues credited to the vote of less than $300 million per year or that have been, for the purposes of this policy, designated as small departments or agencies by the President of the Treasury Board upon recommendation of the Secretary of the Treasury Board. Organizations whose reference levels change so as to bring them above or below the $300 million threshold will not be redefined as large or small departments or agencies unless their reference levels remain above or below the threshold for three consecutive years, to allow for stability and transition, unless otherwise determined by the President of the Treasury Board upon the recommendation of the Secretary of the Treasury Board.

© Her Majesty the Queen in Right of Canada, represented by the President of the Treasury Board, 2017,
ISBN: 978-0-660-09932-3

Date modified: 2018-03-29